Políticas básicas

- Políticas básicas
- Quais são as nossas recomendações?
- Quais são as sugestões?

Políticas básicas

Esta Orientação Técnica estabelece uma política básica de Segurança da Informação em três níveis: o Nível 0 é voltado aos Órgãos Setoriais que não possuem nenhuma política de Segurança da Informação, o Nível 1 se dirige aos que já implantaram o Nível 0 e, por fim, o Nível 2 é voltado aos Órgãos Setoriais que já alcançaram o Nível 1.

Deve-se ressaltar que a política descrita nesta Orientação se limita apenas ao que se entende ser o mínimo indispensável, estando muito longe ainda do ideal. É fundamental que cada Órgão sempre busque enriquecer, expandir e aprimorar a Segurança da Informação dentro da sua organização, para além do disposto nesta Orientação Técnica.

- **NÍVEL 0**

O Nível 0 é voltado aos Órgãos Setoriais que não possuem maturidade suficiente para desenvolver atividades mais específicas de Segurança da Informação, seja por falta de conhecimento, seja por falta de equipe, ou ainda por ser um Órgão Setorial recém-criado e, portanto, ainda em processo de estruturação.

Nesse caso, é importante que o responsável pela Tecnologia da Informação e Comunicação tenha pelo menos algumas
informações rudimentares em mãos. Naturalmente, isso está longe de ser suficiente, necessitando que haja esforços
para aumentar a maturidade do Órgão Setorial em termos de Tecnologia da Informação, de forma a avançar nos níveis da Segurança da Informação.

O Nível 0 exige as seguintes medidas:

Área de Gestão	**Medidas a serem implementadas**
Gestão de Vulnerabilidades e Ameaças	-o-
Monitoramento e Operações	-o-
Infraestrutura e Rede	Limitar o uso de contas de administrador ou similares, bem como privilégios administrativos de acesso/execução, de forma que apenas as pessoas que realmente precisem tenham acesso a essas contas e/ou privilégios. Alterar todas as senhas padrão de infraestrutura e de rede para uma senha mais segura, gerido pelo responsável pela tecnologia da informação e comunicação do Órgão Setorial

Identidades e Acessos	Implantar e manter processos de gestão de identidades e acessos, incluindo a parte de provisionamento, alteração e exclusão. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que são aplicados critérios de senha, para se ter senhas adequadamente fortes. Restringir as contas privilegiadas de usuário, tais como as contas de administrador, root e equivalentes, para que apenas os usuários que necessitam tais contas por necessidade de serviço, ou usuários que sejam servidores de carreira ou especialização em tecnologia da informação, possam ter permissão de uso de tais contas. Definir processos de concessão e revogação de acesso, podendo incluir a necessidade de assinatura de um termo de responsabilidade.
Nuvem	Considerar, como padrão, que os dados na nuvem devem estar armazenados em território brasileiro.
Endpoints e Dispositivos Móveis	Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que está acontecendo a aplicação de patches do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que há a proteção de endpoints, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos um antivírus. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que foram implantados para rede wireless, configurando no mínimo o protocolo WPA2. Alterar todas as senhas padrão das contas de administrador ou equivalentes para uma senha mais segura, gerida pela equipe de tecnologia da informação e comunicação do Órgão Setorial. Implantar um sistema de gestão de ativos para gerir os endpoints.
Dados e Aplicações	Localizar onde estão os dados mais críticos armazenados pelo Órgão Setorial e, se estiverem armazenados em equipamentos pessoais, ter pelo menos uma cópia atualizada periodicamente em um repositório corporativo do Órgão. Implantar infraestrutura e rotinas básicas de backup de dados, considerando a Orientação Técnica sobre o tema. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que há controles de acesso às bases de dados do Órgão Setorial, de forma que o acesso seja estritamente em função das necessidades de serviço.

- **NÍVEL 1**

O Nível 1 se destina aos Órgãos Setoriais que já iniciaram um processo de desenvolvimento e amadurecimento da
sua equipe de Tecnologia de Informação e Comunicação. O objetivo é começar a munir a equipe com conhecimentos e ferramentas para atuarem de forma mais presente.

Além do Nível 0, o Nível 1 exige também as seguintes medidas:

Área de Gestão	**Medidas a serem implementadas**
Gestão de Vulnerabilidades e Ameaças	-o-
Monitoramento e Operações	-o-
Infraestrutura e Rede	Implantar medidas de segurança física para proteger no mínimo a infraestrutura principal de tecnologia da informação e comunicação do Órgão Setorial, incluindo[6]: • **Porta com chave/cadeado que esteja efetivamente operacional.** • **Claviculário ou equivalente para guardar as chaves, incluindo as chaves dos racks.** • **Limitação do acesso físico à infraestrutura principal apenas às pessoas que efetivamente trabalham com os ativos localizados na mesma.**
Identidades e Acessos	Definir papéis para padronizar os conjuntos de permissões de acesso, ao invés de definir acessos para cada usuário, documentando os papéis definidos e mantendo a documentação no repositório de dados corporativo do Órgão Setorial. Aplicar critérios de senha, para se ter senhas adequadamente fortes.
Nuvem	-o-

Endpoints e Dispositivos Móveis	Gerir a aplicação de patches do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas. • **Avaliar também a possibilidade de utilizar o servidor WSUS do Integrador Estratégico ou até mesmo ter um servidor WSUS interno ao Órgão Setorial, de forma a evitar congestionamento de rede.** Implantar a proteção de endpoints, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos: • **Anti-malware, incluindo antivírus;** • **Firewall;** • **Filtro para navegação Web, que pode ser implantado tanto por meio de uma solução centralizada quanto por meio de add-ons de navegadores;** • **Detector de comportamento suspeito/anômalo.** Implantar e manter mecanismos de segurança para rede wireless, configurando no mínimo o protocolo WPA2.
Dados e Aplicações	Implantar controles de acesso às bases de dados do Órgão Setorial, de forma que o acesso seja estritamente em função das necessidades de serviço. Se o Órgão realizar o desenvolvimento de aplicações, incluir como requisito não funcional a exigência de não inserir segredos (senhas, tokens etc.) no código-fonte, exceto para fins meramente de testes. Se o Órgão realizar o desenvolvimento de aplicações, implantar controle de versão e gestão de repositório de código. Se o Órgão realizar o desenvolvimento de aplicações, incluir no desenvolvimento a geração de logs de auditoria.

6. Por “infraestrutura principal” entende-se o ambiente que se designa informalmente como a “sala de servidores”, contendo os servidores e/ou os ativos de rede principais. Excluem-se os data centers (salas-cofre e infraestrutura associada), pois as exigências nesse caso são diferenciadas e muito mais rigorosas.

- **NÍVEL 2**

O Nível 2 deve incorporar, ainda que em parte, da abordagem baseada em riscos. Para que isso possa ser realizado, o Órgão Setorial deverá ter pelo menos uma pessoa da equipe de tecnologia de informação e comunicação que tenha recebido capacitação formal em análise e gestão de riscos, preferencialmente o líder da equipe de tecnologia de informação e comunicação.

Além do Nível 1, o Nível 2 exige também as seguintes medidas:

Área de Gestão	**Medidas a serem implementadas**
Gestão de Vulnerabilidades e Ameaças	Utilizar ferramentas automatizadas para conduzir, de forma periódica, avaliação básica de vulnerabilidade em sistemas de alto valor que o Órgão disponibiliza na internet.
Monitoramento e Operações	Definir e documentar processos básicos de continuidade de negócios e recuperação de desastres para pelo menos um evento negativo de impacto crítico.
Infraestrutura e Rede	Implantar mecanismos de detecção de ativos não identificados e/ou não autorizados na rede interna. Implantar e manter um ou mais firewalls para controlar o tráfego de rede, especialmente se o Órgão Setorial tiver um link direto para a internet. Implantar e manter uma ou mais VPNs (rede privada virtual), especialmente se o Órgão Setorial utilizar acesso remoto, incluindo a conexão a algum ambiente IaaS. Implantar e manter um sistema de detecção e/ou prevenção a intrusões de rede, preferencialmente como parte de um firewall ou de um produto de gestão unificada de ameaças (UTM). Planejar, implantar e documentar a segmentação/ zoneamento de rede.
Identidades e Acessos	-o-
Nuvem	Investir em capacitação para ganhar conhecimento na avaliação do melhor modelo de contratação/implantação, além de conhecimentos para realizar a contratação em si. Considerar, como padrão, que os dados na nuvem devem estar armazenados em território brasileiro. • **No caso do Órgão Setorial ter um líder de TI com capacitação formal em Gestão de Riscos e/ou uma unidade formalmente constituída de Segurança da Informação, o Órgão poderá armazenar seus dados na nuvem fora do território nacional, mediante análise de risco e justificativa.**

Endpoints e Dispositivos Móveis	Implantar um sistema e/ou um processo de gestão de licenças de software, incluindo um processo contínuo de adequação e atualização planejada das licenças. Realizar um processo de hardening[7] (melhoria de robustez dos endpoints) de acordo com boas práticas conhecidas, tais como: • **Utilizar guias, checklists ou benchmarks amplamente utilizadas pelo mercado para ter um ponto de partida de realização de hardening;** • **Utilizar imagens atualizadas para instalar nos endpoints, se possível já após um processo de hardening da imagem;** • **Limitar os privilégios das contas de administrador ou root local e/ou as pessoas com acesso a essas contas.**
Dados e Aplicações	Se o Órgão realizar o desenvolvimento de aplicações, mapear as dependências da segurança da aplicação em termos de infraestrutura. Se o Órgão realizar o desenvolvimento de aplicações, incorporar um mecanismo ou processo de teste de segurança de aplicações dentro da etapa de testes do ciclo de desenvolvimento de aplicações. Se o Órgão disponibiliza aplicações para a internet que são hospedadas dentro da sua própria infraestrutura, implantar uma WAF (Web Application Firewall).

7. Alguns exemplos possíveis:
https://nvd.nist.gov/ncp/repository
https://iase.disa.mil/stigs/Pages/a-z.aspx
https://github.com/nsacyber/Windows-Secure-Host-Baseline
http://www.buffalo.edu/content/dam/www/ubit/docs/guidance-documents/appendix-a-server-security-checklist.pdf

Para o caso específico do Nível 2, o líder da unidade formalmente constituída para gerir a tecnologia de informação e comunicação do Órgão Setorial poderá estabelecer um plano de adoção gradual das medidas descritas, considerando-se questões de caráter técnico, de pessoal e orçamentário/financeiro.

Em caso de ter alguma prática ou controle listados acima que exijam tecnologia e/ou processo que o Órgão Setorial ainda não detém, o líder poderá realizar e executar um planejamento, refletido no Plano Diretor Setorial de Tecnologia da Informação e Comunicação e limitado à disponibilidade orçamentária, para adquirir e/ou desenvolver tal tecnologia, bem como desenvolver e internalizar os processos necessários.

Em termos de Escala de Maturidade, a aplicação comprovada da política em Nível 1 habilita o Órgão Setorial a pleitear a medalha de bronze em Política de Segurança da Informação

Quais são as nossas recomendações?

- Para um Órgão Setorial sem nenhuma política de Segurança da Informação publicada ou publicizada, implantar a política em Nível 0 desta Orientação, seguindo-se o checklist disponível no Anexo.
- Para um Órgão Setorial que já implantou a política em Nível 0, buscar a implantação do Nível 1.
- Para um Órgão Setorial que já implantou a política em Nível 1, buscar a implantação planejada e gradual do Nível 2, considerando-se as capacidades e necessidades técnicas, de pessoal e de orçamento.
- Se o Órgão já alcançou o Nível 2, buscar aprimorar e expandir os seus controles de segurança para melhor gestão da Segurança da Informação.

Quais são as sugestões?

- Automatizar os procedimentos de dimensionamento e alocação de infraestrutura.
- Incorporar os requisitos de segurança dentro do processo de desenvolvimento ou do termo de referência de aquisição da aplicação.